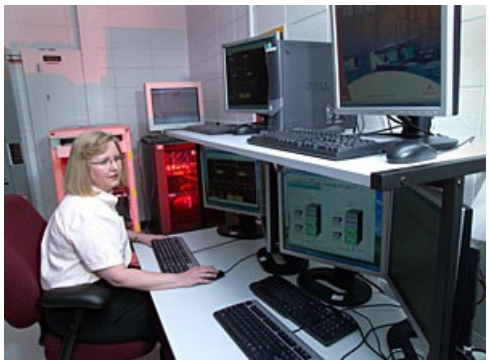
INL increases infrastructure security at SCADA summit

When a virus, worm or spyware makes its way through your firewall and brings your e-mail and Web browsing to a grinding halt, it can be frustrating. But when that same virus penetrates a computer control system operating a critical infrastructure like the electric power grid, it becomes a matter of national security.

Faced with this growing concern, scientists and engineers at Idaho National Laboratory are tackling infrastructure cyber security head-on by developing new technologies, security training and tools to increase the resiliency of the nation's critical infrastructures.

Many modern infrastructures rely on sophisticated computer-based components to operate circuit breakers on the power grid or monitor pumps and valves that change the flow of water at dams. These process control systems were originally designed before the emergence of the Internet and were built to be isolated, non-networked environments, therefore lacking security features like firewalls, encryption or antivirus software.

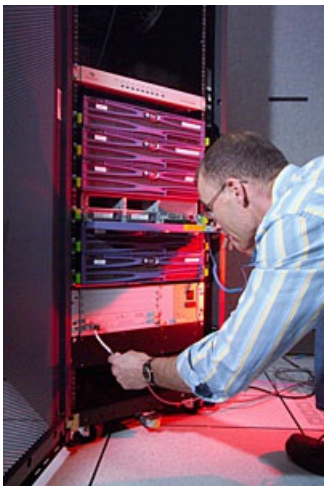
Today, however, many of these computer control systems have been networked to the public Internet to provide users efficient services, lower prices and instant access to data. This connectivity makes them vulnerable to cyber threats such as viruses, worms and deliberate intrusions by hackers or terrorists.



INL researcher Kathy Lee analyzes a prototype SCADA system inside INL's SCADA Test Bed.

One of the most popular computer infrastructure systems, SCADA (Supervisory Control and Data Acquisition) is commonly found in sectors such as electric power and the oil and gas industries. Once deployed, SCADA systems must operate continuously, sometimes for 30 or 40 years, to provide a constant supply of power and services. This continuity of service makes installing patches and fixing software glitches more difficult because these systems never shut off and are generally too expensive to have backup systems in place.

To address these infrastructure security issues, 25 INL cyber and critical infrastructure protection researchers will travel this week to Las Vegas, Nev., to instruct executives and chief security officers from major utilities on how to better protect their computer-based control systems. The training courses are part of the Process Control and SCADA Summit sponsored by the SANS Research Institute, a Maryland-based leader in information security training and certification.



INL engineer Don Dudenhoeffer examines a SCADA vendor's system inside INL's SCADA Test Bed.

During the three-day summit, INL researchers will provide comprehensive, hands-on cyber security and control systems training to more than 200 utility engineers and equipment manufactures from the United States and several foreign countries. The training classes range from introductory classes for managers to complex courses requiring thorough knowledge of working control systems. The training is provided free of charge to attendees by the Department of Energy and the Department of Homeland Security.

INL researchers will teach five different training courses and make presentations at 11 panel sessions with topics ranging from Control Systems Security Innovations to Vulnerability Mitigation and Measurement.

In March, INL cyber security researchers provided similar control systems security training to more than 300 utility executives at the first Process Control and SCADA Summit in Orlando, Fla. During the summit, Rep. Dan Lungren of California, a member of the U.S. House Homeland Security Committee, awarded several companies and agencies, including INL, DOE and DHS, with SCADA Leadership Awards.

In April, SCADA Summit organizers teamed up with several industry and government researchers, including INL, the New York State Office of Cyber Security and Critical Infrastructure and the SANS Institute, to establish the SCADA Procurement Project, which will assist critical infrastructure utilities and manufacturers in the development of common security requirements and a collective buying power to ensure that minimum security standards are incorporated into all future SCADA systems that currently lack federal regulation.

This week's summit runs from Sept. 28 to 30. More information can be found at www.sans.org/scadasummit_fall06

General Contact:
Communications,

Feature Archive